# Department of Homeland Security Daily Open Source Infrastructure Report for 14 July 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

**Daily Highlights**

- The Casper Star−Tribune reports the Wyoming Infrastructure Authority has drawn a map identifying strategic energy corridors where huge new electrical transmission lines could boost the state's role as a major energy supplier to the West. (See item 4)
- The Associated Press reports the National Transportation Safety Board is investigating the possibility that lithium batteries aboard a UPS cargo plane ignited, causing the aircraft to catch fire. (See item 14)
- Massachusetts officials have ordered every road and tunnel in the city highway system to be examined after inspectors found at least 60 more trouble spots in the Big Dig tunnel, where a woman was crushed to death by three−ton ceiling tiles on Monday, July 10. (See item 15)



## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 14, Press & Sun−Bulletin (NY)* — **Rapidly rising water left power plant in dark.** AES Westover, a 126−megawatt coal−fired electric generation station, came within four feet of complete and utter destruction on June 28. The plant suffered millions of dollars in water damage, and will be shut until at least the end of July and possibly through mid−August. The

toll of destruction is staggering: pumps, compressors, 100 motors, hundreds of junction boxes and thousands of circuit boards were lost or damaged when floodwaters poured into the plant that sits on the east bank of the Susquehanna River. In a matter of hours, the river and nearby creek spilled over their banks, barely giving the crew time to shut the plant down. Whole sections of the plant must now be replaced. The shutdown comes at a critical time for the plant, when electricity is at peak demand during the hottest part of summer. Ken Klapp, a spokesperson for the agency that operates New York's electric grid, downplayed the severity of losing AES Westover generation. It represents less than 0.5 percent of last year's total peak demand. He said if the plant were closer to the New York metropolitan region, the loss would have been far more critical.
Source: http://www.pressconnects.com/apps/pbcs.dll/article?AID=/20060711/NEWS01/607110318/1006

2. *July 13, Reuters* — **Oil hits record near $76 on Nigeria, Mideast.** Oil surged to a record high near $76 a barrel on Thursday, July 14, on renewed worries over supply from major exporter Nigeria and as conflict between Israel and Hizbollah in Lebanon heightened international tensions. Prices also rose as the Iran nuclear row appeared to be heading to the United Nations Security Council, North Korea walked out of talks with South Korea, and crude inventories in top consumer the United States fell more than expected. U.S. crude traded 80 cents higher at $75.75 a barrel, after hitting a record $75.89. In Nigeria, two suspected explosions at a crude oil pipeline operated by Agip caused oil spills, Nigerian officials said. Royal Dutch Shell Plc has already had to shut down 473,000 barrels per day of Nigerian supply, almost a quarter of output in Africa's top oil supplier, due to attacks by rebels. Supply breaks and growing Middle East tension mean oil prices may rise further, analysts say.
Source: http://www.nytimes.com/reuters/business/business-markets-oil.html?_r=1&oref=slogin

3. *July 12, Associated Press* — **Citgo to cut off gasoline shipments to U.S.** The Citgo Petroleum Corp. has announced it will no longer sell gasoline to roughly 1,800 U.S. stations, forcing the owners of some stations to find other suppliers. While it may create some logistical headaches for gasoline retailers in the short term, the move should not have any impact on the nation's overall fuel supply. The company has decided to sell to retailers only the 750,000 barrels a day that it produces at three U.S. refineries in Lake Charles, LA, Corpus Christi, TX, and Lemont, IL. Over the next year Citgo will cease distributing gasoline in 10 states and stop supplying some stations in four additional states, Citgo spokesperson Fernando Garay said Wednesday, July 12. The states where Citgo will stop selling gasoline are: Iowa, Kansas, Kentucky, Minnesota, Missouri, Nebraska, North Dakota, Ohio, Oklahoma, and South Dakota. A limited number of stations in Illinois, Texas, Arkansas, and Iowa will also be affected.
Source: http://kutv.com/topstories/local_story_193161040.html

4. *July 12, Casper Star-Tribune (WY)* — **Wyoming maps energy corridors.** Wyoming energy officials have drawn a map identifying routes where huge new electrical transmission lines could boost the state's role as a major energy supplier to the West and the rest of the nation. The Wyoming Infrastructure Authority released maps this week detailing strategic energy corridors based on several pending transmission deals. The mapping was done in partnership with National Grid USA and builds on work done in the Rocky Mountain Area Transmission Study, which identified several potential transmission pathways to link Wyoming to Western markets.

Wyoming's effort parallels the federal government's West−Wide Energy Corridor effort to identify wire and pipeline corridors throughout 11 Western states. The new maps are also part of a continuing effort toward completing at least three major power lines from Wyoming to California, Colorado's Front Range, and Arizona.
Source: http://www.casperstartribune.net/articles/2006/07/12/news/top_story/a732e70a12d1fa37872571a8007f13ee.txt

5. *July 12, Federal Energy Regulatory Commission* — **Testimony: Federal Energy Regulatory Chairman testifies on summer electric reliability issues.** On Wednesday, July 13, the House Government Reform Subcommittee on Energy and Resources conducted an oversight hearing entitled, “Can the U.S. Electric Grid Take Another Hot Summer?” The hearing examined electricity reliability issues highlighted in the Federal Energy Regulatory Commission’s Summer Energy Market Assessment 2006 which notes four major geographical areas with potentially critical electricity supply issues: Southern California; Long Island; New York; and Ontario, Canada, which affects U.S. states in the Great Lakes region and Southwest Connecticut.
Testimony: http://www.ferc.gov/EventCalendar/Files/20060712145318−kelliher−test−07−12−06.pdf
Summer Energy Market Assessment 2006: http://www.ferc.gov/EventCalendar/Files/20060518103507−A−3−w ith−talking−ptsl.pdf
Source: http://www.ferc.gov/EventCalendar/EventDetails.aspx?ID=2749&CalType=%20&CalendarID=116&Date=&View=List

[Return to top]

## Chemical Industry and Hazardous Materials Sector

6. *July 13, Hattiesburg American (MS)* — **Acid spill disrupts traffic.** Emergency workers shut down a 1−mile section of U.S. 98 near Bellevue, MS, to traffic Wednesday, July 12, after hydrochloric acid spilled from a container inside a truck headed to Lumberton. "We are taking all precautions to protect people," James Smith, Lamar County emergency management director, said Wednesday, as dozens of local and state officials manned roadblocks, oversaw cleanup of the hazardous chemical and directed residents through a detour route. No one was hurt in the incident in which 300 to 500 gallons of acid leaked from a container inside a SAIA truck, Smith said. Hydrochloric acid is a strong, highly corrosive acid widely used in cleaning metals. The hydrochloric acid, which leaked onto the trailer bed before spilling into the dirt beside the road, appeared slightly yellow where it had burned the green grass and turned it brown. U.S. Environmental Services of Jackson used lime to neutralize the acid and decontaminate the truck. Another truck was being brought in to collect the remaining acid from the trailer.
Source: http://hattiesburgamerican.com/apps/pbcs.dll/article?AID=/20060713/NEWS01/607130304/1002

7. *July 12, WMUR 9 (NH)* — **Homes evacuated after chemical release.** Two people in New Ipswich, NH, were taken to a hospital and some homes were evacuated Wednesday, July 12, after a hazardous chemical was released at a business. Officials said that nitric acid was released when a chemical came into contact with metal at Warwick Mills. As a precaution, the

business and nearby homes were evacuated while the chemical dissipated. Officials said they believe the chemical had dissipated, but they were waiting for air−quality readings.
Source: http://www.wmur.com/news/9505694/detail.html

[Return to top]

## Defense Industrial Base Sector

8. *July 12, Federal Computer Week* — **Clearance process accelerates into high gear.** Federal security officials insist they are moving ahead rapidly with new policies and procedures that will break the logjam of security clearance applications and improve the timeliness and efficiency of background investigations. Although the Intelligence Reform and Terrorism Prevention Act of 2004 mandated a thorough overhaul of the system, which critics have called a relic of the Eisenhower administration, agencies have been slow to respond. The situation gained renewed attention in May when the Defense Security Service halted the security clearance process because it lacked funds. “We are going to reform the security clearance function,” said Clay Johnson, deputy director for management at the Office of Management and Budget(OMB). Johnson, speaking Tuesday, July 11, to an audience of contractors and vendors at OMB, said the agency has a clear definition of success that it will evaluate each December from 2006 to 2009, the benchmarks established by the intelligence reform act.
Source: http://www.fcw.com/article95238−07−12−06−Web

[Return to top]

## Banking and Finance Sector

9. *July 13, VNUNet* — **Phishers crack two−factor authentication.** Security experts have detected a new type of phishing attack that could render two−factor authentication useless. A dual−factor security system typically uses a password and some kind of hardware security device such as a smartcard or token that issues temporary passwords. The Security Fix blog reported that researchers at Secure Science Corporation spotted a phishing Website targeting Citibank's Citibusiness service that attempted to steal both the user name and password as well as the temporary password issued by the security token. The site furthermore acted as a middleman that relayed the information to the Citibank server for authentication. It prompted users if the information they entered was incorrect.
Source: http://www.vnunet.com/vnunet/news/2160250/phishers−crack−two −factor

10. *July 13, Computing (UK)* — **Mobiles set for key role in card authentication.** Mobile phones could be used to authenticate financial transactions in the UK, says the head of financial crime at Lloyds TSB. South Africa’s First National Bank and two banks in New Zealand are already using SMS to deliver authentication codes, but Lloyds TSB’s Ken Farrow says the phone is set to become the actual card−reading device. He believes mobiles are perfectly suited for two−factor authentication because people carry the devices with them all the time. While development of two−factor phones has not yet started, UK payments industry association Apacs has held discussions with mobile phone companies. Richard Martin of Apacs believes phones will be used to authenticate transactions, but contactless technology is more viable. Tim

Pickard of RSA Security thinks mobile phone card readers make sense from a convenience point of view, but advocates standardization so that all cards can be read.
Source: http://www.computing.co.uk/computing/news/2160284/mobiles−se t−key−role−card

11. *July 12, U.S. Department of the Treasury* — **Treasury identifies money laundering cell of the Arellano Felix Organization.** The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Wednesday, July 12, identified 34 companies and individuals associated with two Mexican drug cartels, the Arellano Felix Organization (AFO) and the Arriola Marquez Organization. One OFAC action targets an Arellano Felix Organization money laundering cell, run by key individual Lorenzo Arce Flores, comprised of 14 companies and 15 individuals located in Tijuana, Baja California, Mexico. Another OFAC action identifies five individuals who are financial operatives of the Arriola Marquez Organization in the state of Chihuahua, Mexico. Lorenzo Arce Flores is a key AFO money launderer. Arce Flores directs an operation which facilitates money laundering and bulk smuggling of cash across the border. OFAC has identified several Mexican money service businesses that are part of the Arce Flores network, including Caja Amigo Express S.A. DE C.V., Operadora De Caja Y Servicios S.A. De C.V., Multicaja De Tijuana S.A. De C.V., and Profinsa. A Mexican armored car company, Strong Link De Mexico S.A. De C.V., is also named as part of this money laundering operation.
Source: http://www.ustreas.gov/press/releases/hp08.htm

12. *July 12, Hardware Zone* — **Trend Micro warns against spy−phishing.** Trend Micro warns Internet users against spy−phishing, an emerging crimeware technique which capitalizes on the increasingly popular trend of blended threats. Spy−phishing, Trend Micro believes, is the next step for phishers and spyware authors who want to steal money and personal information from users. Some malware writers create spyware programs to steal credit card numbers, account log−ins, or a variety of other types of personal information. Others phish for personal information either to use for themselves or to sell to others. "Spy−phishing...uses phishing techniques to initially present itself to users, then typically engages a host of other techniques and exploits to surreptitiously download and install spyware applications in the background." According to data collected by Trend Micro, the amount of Trojan spyware such as that employed in spy−phishing attacks has been steadily increasing.
Source: http://www.hardwarezone.com/news/view.php?id=4939&cid=8

13. *July 11, Sophos* — **Widespread Gmail phishing email lures with $500 cash prize.** Experts at SophosLabs have warned of a widespread phishing e−mail campaign that tries to trick users out of money by pretending to be a random cash prize from Gmail, Google's popular free e−mail service. The e−mails claim that the recipient has been randomly selected for a $500 cash prize, and that the money can be automatically paid to them if they click on the embedded Web link. The link users are told to click on pretends to be a legitimate Gmail link, but really points to a bogus Tripod−hosted Website. The fake Web page says that there has been a problem sending the payment, and asks victims to enter their details and pay a membership fee of $8.60.
Source: http://www.sophos.com/pressoffice/news/articles/2006/07/gmai lphish.html

[Return to top]

## Transportation and Border Security Sector

**14.** *July 13, Associated Press* — **NTSB probes laptop batteries in jet fire.** Did laptop batteries aboard a UPS cargo plane ignite, causing the aircraft to catch fire? The National Transportation Safety Board (NTSB) began looking into the question at a hearing Wednesday, July 12. All three crewmembers on the cargo plane were treated for minor injuries after it made an emergency landing shortly after midnight February 8, at Philadelphia International Airport. Several other incidents have occurred in recent years in which lithium batteries −− used in laptops and cell phones −− have caught fire aboard airplanes. Less than two months ago in Chicago, a spare laptop battery packed in a bag stored in an overhead bin started emitting smoke, chief crash investigator Frank Hilldrup of the NTSB testified. In 1999, a shipment of lithium batteries ignited after it was unloaded from a passenger jet at Los Angeles International Airport. Another shipment erupted into flames in Memphis in 2004 when it was being loaded onto a FedEx plane bound for Paris. The NTSB is also examining other related issues, such as what can be done to make cargo flights safer and the overall emergency response to the incident.
Source: http://biz.yahoo.com/ap/060713/pa_cargo_plane_fire.html?.v=1

**15.** *July 13, San Francisco Chronicle* — **Boston highway roads and tunnels to be checked.** Massachusetts officials have ordered that every road and tunnel in the city highway system should be examined after inspectors found at least 60 more trouble spots in the Big Dig tunnel where a woman was crushed to death by three−ton ceiling tiles on Monday, July 10. Michael Lewis, the project director for the Big Dig, said bolts appear to be loose, that gaps exist, or that other parts of the ceiling seem compromised in at least 60 places in the eastbound tunnel. In addition, the Massachusetts attorney general, Thomas Reilly, said problems with ceiling anchor bolts in the tunnel had been identified in 1999, when the ceiling was built, and that his office was investigating to see whether a plan to correct those problems was carried out. Matthew Amorello, chairman of the Massachusetts Turnpike Authority, ordered an evaluation of the entire highway system in the Boston area, even roads and tunnels that are not part of the Big Dig. The tunnel, known as the Interstate 90 connector because it links the Massachusetts Turnpike and Interstate 93 with the Ted Williams Tunnel and I−90, is a major route to Boston's Logan International Airport.
Source: http://www.sfgate.com/cgi−bin/article.cgi?file=/c/a/2006/07/ 13/MNG20JU7DI1.DTL

**16.** *July 13, Chicago Tribune* — **Canine works for Chicago Transit Authority.** The first police dogs the federal government has trained to sniff out explosives on mass−transit systems have started working at the Chicago Transit Authority and nine other bus and train agencies in the United States. The dogs, schooled at a U.S. military base, are scheduled to complete their local certification about the time of the fifth anniversary of the September 11, 2001 terrorist attacks. The effort is part of a multi−layered strategy to elevate security levels for transit commuters to those comparable to airlines following the 9/11 hijackings. Homeland security officials have warned U.S. transit agencies to remain vigilant as the anniversary approaches. Experts say the threat of a mass−transit attack succeeding is high because the systems are accessible to everyone, much more difficult to secure than airports and, as potential targets, offer terrorists the ability to cause widespread mayhem and fear. The dogs and their police handlers recently graduated from the Transportation Security Administration's explosives−detection program at Lackland Air Force Base, near San Antonio. Lackland could be considered the Harvard of bomb−sniffing schools, also training military canines to work alongside U.S. soldiers in Iraq and Afghanistan.

Source: http://www.chicagotribune.com/news/local/chi−0606120105jun12,1,5525445.column?coll=chi−news−hed

17. *July 12, United Press International* — **Mouse infestation alleged on airplane.** Aircraft overhaulers in Kansas City say an American Airlines Boeing 767 that came in for servicing in April was infested with mice. KSDK−TV in St. Louis said a longtime employee at the overhaul base at Kansas City International Airport contacted the TV station about the problem. Workers found nests in air vents and dead mice in emergency oxygen masks. The mice ate insulation and chewed through wires. KSDK−TV said exterminators estimated that anywhere from 900 to 1,000 mice could be on the aircraft. American Airlines disputes that number, saying it found only 17 live mice. The Federal Aviation Administration says all insulation and oxygen masks on the plane have been replaced, the cargo bins have been removed and replaced and the wiring has been inspected.
Source: http://www.upi.com/NewsTrack/view.php?StoryID=20060712−11175 0−9962r

18. *July 10, Financial Times/MSNBC* — **Foreign bidders to dominate sale of Midway Airport.** Chicago expects overseas bidders to dominate next year's sale of the city's Midway Airport. The long−term lease of Midway is the latest initiative by Chicago to plug its budget gap following the $1.83 billion sale of a toll road, and will be closely watched by other U.S. cities and states facing a fiscal squeeze caused by rising pension deficits. Dana Levenson, Chicago's chief financial officer, said the city hoped to review initial proposals in September. "We are seeing interest from more than the usual four or five [companies] −− the British, Australian, Singaporean, Germans, and the Spanish," Levenson said. The city has started talks with the Federal Aviation Administration and carriers operating out of Midway. The airport is smaller than the city's main hub, O'Hare, but handled almost 18 million passengers last year and is now one of the largest bases for Southwest Airlines. Airports are almost exclusively owned by cities or other local authorities, though many services are contracted out to the private sector.
Source: http://msnbc.msn.com/id/13803971/

[Return to top]

## Postal and Shipping Sector

19. *July 11, DM News* — **USPS offers final rule on EVS for Parcel Select mailings.** The U.S. Postal Service (USPS) published a final rule July 10 on standards that it will adopt to implement the Electronic Verification System (EVS) for certain Parcel Select mailings. The EVS eliminates the current paper−driven and manual processes used to verify such mailings. The rule was published in the Federal Register. EVS will be required beginning August 1, 2007. The USPS said this time period will provide mailers and shippers with sufficient time to meet standards and to perform the testing necessary for satisfactory operations. The required change will also extend to Standard Mail machinable parcels and parcels from other Package Services subclasses (Bound Printed Matter, Library Mail, or Media Mail) with permit imprint Parcel Select parcels. Current procedures for accepting and verifying parcel mailings are paper−driven and can be challenging for the shipping industry, the USPS said.
Source: http://www.dmnews.com/cms/dm−news/direct−mail/37428.html

[Return to top]

# Agriculture Sector

**20.** *July 13, Agence France−Presse* — **Suspected case of mad cow disease in Slovenia.** A suspected case of mad cow disease has been found in Litija, about 20 miles east of the capital Ljubljana, Slovenian veterinary authorities have announced. "The suspected case was detected in a cow that was slaughtered on Tuesday, July 11, on a farm in Litija," Slovenia's veterinary office said in a statement, adding the five−year−old cow had been born and bred in Slovenia. Samples have been sent for additional testing. So far five cases of bovine spongiform encephalopathy, also known as mad cow disease, have been detected in Slovenian−born cows and one in an imported cow.
Source: http://news.yahoo.com/s/afp/20060713/hl_afp/sloveniahealthmadcow_060713143349;_ylt=AkFFOMyBwH9yYIrNKjUATTaJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

**21.** *July 12, U.S. Department of Agriculture* — **Guide to help agricultural producers protect the food supply.** The U.S. Department of Agriculture (USDA) Wednesday, July 12, released a guide entitled "Pre−Harvest Security Guidelines and Checklist 2006" to help agricultural producers enhance security at the farm level. These practical measures help to protect against natural disasters, as well as the unintentional or intentional introduction of plant or animal diseases. The voluntary guidelines and checklists were developed based upon recommendations made by producers throughout the U.S. Guidelines have been developed for general agriculture; dairy; crops; cattle and poultry security. USDA's local Farm Service Agency Service Centers are distributing the "Pre−Harvest Security Guidelines and Checklist 2006" to agricultural producers throughout the country.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/07/0245.xml

**22.** *July 12, Animal and Plant Health Inspection Service* — **Screwworm facility inaugurated.** U.S. Department of Agriculture (USDA) representatives joined Panamanian President Martin Torrijos, U.S. Ambassador to Panama William Eaton and Panamanian agriculture officials to inaugurate the soon−to−be−completed Panama Mass Rearing and Research Facility devoted to studying and producing New World screwworms, Cochliomyia hominivorax (Coquerel). The center will be jointly run by USDA's Animal and Health Inspection Service and the U.S.−Panamanian Commission for the Eradication and Prevention of Screwworms, also known as COPEG (Comisión Panamá−Estados Unidos para la Erradicación y Prevención del Gusano Barrenador del Ganado). Scientists with USDA's Agricultural Research Service will be located in the new facility to provide continuing research support. Screwworm eradication efforts save U.S. livestock producers at least $900 million annually. Screwworm is a parasite that affects mammals. Screwworm larvae hatch from eggs laid by flies on host animals and feed on their flesh, causing great suffering and losses.
Source: http://www.aphis.usda.gov/newsroom/content/2006/07/panama_screwworm_vs.shtml

**23.** *July 12, Pennsylvania Department of Agriculture* — **Agriculture Department closes live bird market in Philadelphia.** As a routine precaution, the Pennsylvania Department of Agriculture temporarily closed a live bird market in Philadelphia Wednesday, July 12, after birds tested positive for a strain of avian influenza. Mild cases of avian influenza are routinely discovered in

Pennsylvania and surrounding states. The virus for this particular bird market was discovered during a routine surveillance and does not cause bird or human illness. The Department of Agriculture will investigate all distribution channels of the birds as they traveled to and from the market, to ensure isolation of all sources of the virus. Pennsylvania leads the nation in avian influenza surveillance, testing more than 240,000 samples each year. If a bird tests positive for avian influenza, the flock is immediately quarantined.
Source: http://www.agriculture.state.pa.us/agriculture/cwp/view.asp? A=390&Q=140472

[Return to top]

## Food Sector

Nothing to report.
[Return to top]

## Water Sector

**24.** *July 13, San Francisco Chronicle* — **Greenery using more of state's water.** Home landscaping, particularly lawns, will use an increasingly burdensome amount of water in California over the next 25 years unless big changes are made, according to a new report by the Public Policy Institute of California. The state is expected to add 11 million new residents by 2030, and at least half are expected to locate in hotter, inland areas where single−family homes with lush lawns are popular, according to the report. Landscaping currently accounts for at least half of all residential water demand, according to the report. Without new conservation efforts, the amount of water going to outdoor landscaping is predicted to rise by 1.2 million acre feet a year −− enough to serve roughly 4.8 million people. California cities and suburbs currently use about nine million acre−feet of water a year.
Report: http://www.ppic.org/content/pubs/cep/EP_706EHEP.pdf
Source: http://sfgate.com/cgi−bin/article.cgi?f=/c/a/2006/07/13/BAGI DJU67C1.DTL

[Return to top]

## Public Health Sector

**25.** *July 13, Reuters* — **Multiple mutations in Indonesian bird flu strain.** Multiple mutations have been found in the H5N1 bird flu virus that killed seven family members in Indonesia although scientists are unsure of their significance. An analysis of virus samples from six of the eight members of the family showed 32 mutations accumulated as it spread. The analysis had been presented by virologist Malik Pereis of the University of Hong Kong at a closed meeting of animal and human health experts in Jakarta, Indonesia. Virologists said part of the reason the significance of the mutations is unclear is because withholding the information has hampered the study of the virus.
Research: http://www.nature.com/nature/journal/v442/n7099/full/442114a .html
Source: http://thestar.com.my/news/story.asp?file=/2006/7/13/worldup dates/2006−07−13T163455Z_01_NOOTR_RTRJONC_0_−259426−1&sec=Wo rldupdates

**26.** *July 11, Associated Press* — **State biologists testing migratory birds for avian flu.** Hundreds of Canada geese and other migratory birds are being captured and tested for avian flu by Maine state biologists. The testing of Canada geese, Arctic terns, common eiders and black guillemots by state Inland Fisheries and Wildlife biologists is being done to check for early signs of the bird flu virus before it channels over to Maine's commercial bird flock. Biologists may end up testing hundreds if not thousands of birds before the program ends later this year. Samples are sent to a lab in Connecticut for testing, and the results are sent to the U.S. Department of Agriculture. Canada geese are a favored choice of birds for testing because they often mingle with other species of migrating birds, according to Michael Schummer, a game bird specialist.
Source: http://pressherald.mainetoday.com/news/state/060711avianflu. shtml

[Return to top]

## Government Sector

**27.** *July 13, Washington Technology* — **New standard proposed for information sharing.** The federal government should develop an "authorized use" standard to improve information sharing against terrorism, according to a new report from the Markle Foundation Task Force on National Security in the Information Age. The 100−page report, Mobilizing Information to Prevent Terrorism, was released on Thursday, July 13, and is the third from the task force addressing how to share information for national−security purposes while also protecting privacy and civil liberties. Under the proposed authorized use standard, access would be granted based on how the information will be used, rather than on nationality or location of collection.
Report: http://www.markle.org/downloadable_assets/2006_nstf_report3. pdf
Source: http://www.washingtontechnology.com/news/1_1/homeland/28931−1.htm

[Return to top]

## Emergency Services Sector

**28.** *July 12, Government Accountability Office* — **GAO−06−954T: Individual Disaster Assistance Programs: Framework for Fraud Prevention, Detection, and Prosecution (Testimony).** Federal agencies spend billions of dollars annually to aid victims of natural and other disasters and acts of terrorism. Managers of federal disaster assistance programs face a dual challenge −− delivering aid as quickly as possible while at the same time ensuring that relief payments go only to those who are truly in need. Due to the very nature of the government's need to quickly provide assistance to disaster victims, federal disaster relief programs are vulnerable to significant risk of improper payments and fraudulent activities. On February 13, 2006, and on June 14, 2006, the Government Accountability Office (GAO) testified concerning extensive fraud, waste, and abuse in the Individuals and Household Program (IHP), a component of the Federal Emergency Management Agency's (FEMA) disaster assistance programs. GAO identified significant internal control weaknesses that resulted in FEMA making tens of thousands of Expedited Assistance payments that were based on bogus registration data. GAO also found numerous other internal control failures in FEMA's IHP disaster assistance program, resulting in an estimate that FEMA made $600 million to $1.4

billion in improper and potentially fraudulent payments to registrants. The purpose of this testimony is to establish a framework for preventing, detecting, and prosecuting disaster assistance fraud.
Highlights − http://www.gao.gov/highlights/d06954thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−954T

29. *July 12, Federal Computer Week* — **Emergency provisions added to Federal Acquisition Regulation.** The Office of Management and Budget announced Wednesday, July 12 the release of Federal Acquisition Regulation Part 18, a FAR addition that includes emergency procurement information in a single source to help agencies effectively respond to emergencies. After Hurricane Katrina struck in August 2005, many department officials were unfamiliar with acquisition flexibility regulations regarding emergency situations. So the Office of Federal Procurement Policy requested a new FAR part that would compile such procedures into one section.
Source: http://fcw.com/article95242−07−12−06−Web

30. *July 11, Honolulu Advertiser (HI)* — **Simulated nuclear explosion planned.** The state of Hawaii plans to hold an exercise in mid−August simulating the explosion of a half−kiloton nuclear device at the entrance of Honolulu Harbor, a mock blast that theoretically would result in 10,000 casualties. Several hundred state and military planners and first responders will take part August 14 to 16 in the exercise. State and federal military command and emergency responders will take part, including U.S. Pacific Command at Camp Smith. Although Honolulu Harbor is the site for the simulated explosion, Bellows Air Force Station will represent "ground zero" for the blast, and several hundred emergency responders will have roles there, including the state Urban Search and Rescue Team to search for casualties, and the Honolulu Fire Department, which will work with the health department's radiological monitoring team, said Edward Teixeira, vice director of state Civil Defense. The exercise will help the state develop a nuclear explosion evacuation plan. Officials said there is a terrorism response plan calling for a collective state and federal response using the powers of the president to declare a disaster.
Source: http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID=/20060711/NEWS08/607110337/1001/NEWS

31. *July 11, Kalamazoo Gazette (MI)* — **Michigan Airport site of mock mishap involving anhydrous ammonia.** Plainwell Municipal Airport in Michigan was the site of a mock disaster over the weekend that involved a bus full of Boy Scouts suffering injuries from a leaking anhydrous ammonia tank. Volunteers spent nearly three hours simulating what might happen if a car crashed into a pickup truck hauling an anhydrous ammonia tank just before a loaded bus traveled down the same road. The drill in the southeastern corner of the airport on Saturday, July 9, involved firefighters from Gun Plain Township, Plainwell and Otsego; amateur radio operators; paramedics from both the Plainwell and Wayland Emergency Medical Services agencies; and drivers with the Allegan County Transportation Agency.
Source: http://www.mlive.com/news/kzgazette/index.ssf?/base/news−18/115263133191200.xml&coll=7

[Return to top]

# Information Technology and Telecommunications Sector

**32.** *July 13, IDG News Service* — **Researcher to show code for 'wormable' Windows flaw.** With security vendors worrying that a recently patched Windows bug may lead to a major worm outbreak, the researcher who discovered the flaw said Wednesday, July 12, that he is weeks away from releasing code that exploits the problem. HD Moore, developer of the Metasploit hacking tool, has developed software that could be used to crash a system that has not received Microsoft's MS06−035 update, released Tuesday. However, the software could not be used to create the kind of self−replicating worm that some vendors see as a possibility, he said. Microsoft's posted the MS06−035 bulletin with information about the flaw: http://www.microsoft.com/technet/security/bulletin/ms06−035. mspx
Source: http://www.infoworld.com/article/06/07/13/HNwormable_1.html

**33.** *July 12, CNET News* — **Adobe fixes PDF reader flaws.** Adobe Systems joined Microsoft on "Patch Tuesday" and delivered fixes for two security flaws in the ubiquitous Adobe PDF reader software. The vulnerabilities affect Adobe's Acrobat and Reader software for both the Windows operating system and Apple Computer's Mac OS, Adobe said in two separate security advisories. If left unpatched, the flaws could put Windows and Mac users at risk of a cyberattack. Adobe recommends using the automatic update facility in its applications to install version 6.0.5 or download and install the update from the Adobe Website: http://www.adobe.com/support/downloads/
Source: http://news.com.com/Adobe+fixes+PDF+reader+flaws/2100−1002_3−6093373.html?tag=nefd.top

**34.** *July 12, CRN* — **Cisco details new VoIP, router vulnerabilities.** Cisco Wednesday, July 12, revealed a pair of vulnerabilities, one in its Unified CallManager 5.0 software, the other in the Web−based interface used to configure Cisco routers. Unified CallManager 5.0, software that handles call processing for Cisco VoIP solutions, has two flaws in its command line management interface that could allow a logged−in administrator to gain root access privileges and execute code, overwrite files, and launch denial−of−service attacks, Cisco said. The Unified CallManager 5.0 software, which Cisco upgraded in March to add support for session initiation protocol, also includes a buffer overflow vulnerability that attackers can exploit by placing excessively long hostnames into SIP requests along with malicious code, paving the way for code execution and denial−of−service attacks.
Cisco Security Advisories: http://www.cisco.com/en/US/products/products_security_advisories_listing.html
Source: http://www.crn.com/showArticle.jhtml;jsessionid=ADADGVHOYPMTAQSNDLRSKH0CJUNN2JVN?articleID=190302961

**35.** *July 12, eWeek* — **Critical Excel flaws remain unpatched.** A day after Microsoft shipped a mega−patch to cover eight Excel vulnerabilities, security researchers warn that at least two critical −− and publicly discussed −− flaws affecting users of the spreadsheet program remain unpatched. Proof−of−concept exploit code for both vulnerabilities has been published on the Internet and, in the absence of patches, Microsoft is strongly urging customers to avoid accepting and opening files from untrusted sources. Christopher Budd, a program manager in the Microsoft Security Response Center, confirmed that one vulnerability is caused by a boundary error in a Windows component called "hlink.dll," which can be used to cause a stack−based buffer overflow if an Excel user is tricked into clicking a specially rigged URL in a

malicious Excel document. Budd also confirmed a second unpatched Excel issue that affects certain Asian−language versions of Microsoft Excel.
Source: http://www.eweek.com/article2/0,1895,1988145,00.asp

36. *July 12, Sophos* — **Vladimir Putin death spam helps spread Trojan horse.** Sophos has warned of a spam campaign that poses as a breaking news report from BBC News in an attempt by hackers to infect computer users with a Trojan horse. The e−mail claims that Vladimir Putin, president of the Russian Federation, has died. However, embedded in the HTML e−mail is a hidden script that exploits the ADODB.Stream vulnerability to secretly download the malicious Troj/Dloadr−ZP Trojan horse from a Russian Website. The Trojan horse is designed to download further malicious code which could allow remote hackers to gain unauthorized access to the victim's computer.
Source: http://www.sophos.com/pressoffice/news/articles/2006/07/puti n.html

## Internet Alert Dashboard

**DHS/US−CERT Watch Synopsis**

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US−CERT Operations Center Synopsis:** US−CERT is aware of multiple vulnerabilities in Microsoft Internet Explorer (IE) 6.0. US−CERT is also aware of a public blog that will be posting new web browser bugs on a daily basis in July. US−CERT will be analyzing relevant vulnerabilities, as well as actively monitoring the site to provide additional information as it becomes available. Please review URL: http://metasploit.blogspot.com/2006/07/month−of−browser−bugs .html

US−CERT strongly recommends the following:

Review VU#159220 / Microsoft Internet Explorer vulnerable to heap overflow via the HTML Help Control "Image" property : http://www.kb.cert.org/vuls/id/159220

Disable ActiveX as specified in the following:

Securing Your Web Browser:
http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Malicious Web Scripts FAQ:
http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

Do not follow unsolicited links.

Review the steps described in Microsoft's document to improve the safety of your browser: http://www.microsoft.com/athome/security/online/browsing_saf ety.mspx

US−CERT will continue to update current activity as more information becomes available.

**Public Exploit Code for Unpatched Vulnerabilities in Microsoft Internet Explorer**

US−CERT is aware of publicly available exploit code for two unpatched vulnerabilities in Microsoft Internet Explorer. By persuading a user to double click a file accessible through WebDAV or SMB, a remote attacker may be able to execute arbitrary code with the privileges of the user. US−CERT is tracking the first vulnerability as VU#655100: http://www.kb.cert.org/vuls/id/655100

The second issue is a cross domain violation vulnerability that is being tracked as VU#883108: http://www.kb.cert.org/vuls/id/883108

Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited links.

To address the cross domain violation vulnerability (VU#883108): http://www.kb.cert.org/vuls/id/883108

Disable ActiveX as specified in the Securing Your Web Browser: http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Review Malicious Web Scripts FAQ: http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

US−CERT will continue to update current activity as more information becomes available

**PHISHING SCAMS**

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

**Current Port Attacks**

| | |
|---|---|
| **Top 10 Target Ports** | 1026 (win−rpc), 50497 (−−−), 38566 (−−−), 25 (smtp), 24232 (−−−), 54856 (−−−), 445 (microsoft−ds), 80 (www), 113 (auth), 6881 |

| | |
|---|---|
| | (bittorrent)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

# Commercial Facilities/Real Estate, Monument &Icons Sector

**37.** *July 13, Government Accountability Office* — **GAO−06−614T: Chesapeake Bay Program: Improved Strategies Needed to Better Guide Restoration Efforts (Testimony).** The Chesapeake Bay Program (Bay Program) was created in 1983 when Maryland, Pennsylvania, Virginia, the District of Columbia, the Chesapeake Bay Commission, and the Environmental Protection Agency (EPA) agreed to establish a partnership to restore the Chesapeake Bay. The partnership's most recent agreement, Chesapeake 2000, sets out an agenda and five broad goals to guide the restoration effort through 2010. This testimony summarizes the findings of an October 2005 GAO report (GAO−06−96) on (1) the extent to which appropriate measures for assessing restoration progress have been established, (2) the extent to which current reporting mechanisms clearly and accurately describe the bay's overall health, (3) how much funding was provided for the effort for fiscal years 1995 through 2004, and (4) how effectively the effort is being coordinated and managed. The Government Accountability Office (GAO) made three recommendations in October 2005 to ensure that EPA's Chesapeake Bay Program Office completes its efforts to develop and implement an integrated assessment approach, revises its reporting approach to improve the effectiveness and credibility of its reports, and develops a comprehensive, coordinated implementation strategy that takes into account available resources. GAO is not making any new recommendations in this statement.
Highlights: http://www.gao.gov/highlights/d06614thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−614T

[Return to top]

# General Sector

**38.** *July 13, Associated Press* — **Indian authorities name two suspects in train bombings.** Indian authorities named two suspects Thursday, July 13, in the Mumbai (formerly Bombay) commuter train bombings on Tuesday, July 11. The government's Anti−Terror Squad released photos of two young, bearded men it identified as Sayyad Zabiuddin and Zulfeqar Fayyaz. Their nationalities were not provided. The detentions came as a man claiming to represent al Qaeda said the terror network had set up a wing in Kashmir and praised the attacks. There have been allegations that Islamic militants fighting to wrest predominantly Muslim Kashmir from India have ties to al Qaeda, but Thursday's statement would be the first time Osama bin Laden's network claimed to have spread to Indian territory. Mumbai, a city of 16 million people, was almost back to normal Thursday with tens of thousands of people jamming the commuter train service that was hit by eight bombs, killing at least 200 people and wounding 700.
Source: http://www.usatoday.com/news/world/2006−07−12−india−explosio ns_x.htm

[Return to top]

## DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

### DHS Daily Open Source Infrastructure Report Contact Information

| | |
|---|---|
| Content and Suggestions: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644. |
| Subscription and Distribution Information: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information. |

### Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

### Department of Homeland Security Disclaimer